



Connected Data Privacy Risk and Controls Training Course

14 – 18 December 2026
Milan

Connected Data Privacy Risk and Controls Training Course

Ref: 816_161828 **Date:** 14 – 18 December 2026 **Location:** Milan **Fees:** 5700 Euro

Overview

Connected Data Privacy Risk and Controls Training Course is a five-day intermediate course for privacy, compliance, governance, risk, and operations professionals who leave with a Connected Privacy Control Pack. Participants use connected data privacy, data-flow mapping, privacy risk assessment, privacy by design, data minimization, third-party controls, rights handling, and privacy assurance to protect personal information across digital ecosystems. The course turns fragmented responsibilities into traceable controls. Agile Leaders Training Center develops connected data privacy capability.

Who Should Attend

- Privacy functions responsible for requirements, assessments, rights, and assurance
- Compliance functions responsible for translating obligations into operating controls
- Information governance functions responsible for data inventories, retention, and accountable use
- Risk functions responsible for identifying and treating privacy impacts
- IT governance functions responsible for connected services and external-provider controls
- Business operations functions responsible for data-sharing workflows and evidence

The course assumes participants can document business processes and control responsibilities, and leaves out legal certification preparation, software engineering, penetration testing, and technical incident forensics.

Departments and Industries

The course supports departments and industries that process personal or sensitive information across connected services and partner relationships.

- Privacy, compliance, risk, legal operations, information governance, and internal audit departments
- Banking, insurance, healthcare, telecommunications, and digital-platform services
- Retail, hospitality, transportation, education, and professional services
- Cloud-enabled operations, connected-product teams, and shared-service organizations
- Public services, utilities, and regulated business operations

Learning Objectives

By the end of this course, participants will be able to:



- Apply privacy-risk methods to connected data flows
- Build inventories, role maps, and lifecycle control records
- Analyze purpose, minimization, access, retention, and sharing decisions
- Evaluate privacy-by-design and third-party safeguards
- Prioritize rights, incident, assurance, and remediation actions
- Build a Connected Privacy Control Pack

Course Agenda

Day 1: Map the Connected Data Ecosystem

- Personal Data Processing Lifecycle Map
- Connected Service and Device Inventory
- Controller, Processor, and Partner Role Matrix
- Purpose and Data-Use Statement
- Data Flow and Transfer Diagram

Day 2: Assess Privacy Risks

- NIST Privacy Framework Current Profile
- Privacy Risk and Impact Assessment Canvas
- Individual Harm and Business Impact Register
- Data Minimization and Necessity Test
- Connected Processing Risk Prioritization Matrix

Day 3: Design Lifecycle Controls

- Privacy-by-Design Requirement Checklist
- Default Settings and Selective Collection Review
- Access, Disclosure, and Sharing Control Matrix
- Retention and Disposal Decision Schedule
- Product Change Privacy Gate

Day 4: Govern Partners and Operations

- Third-Party Privacy Requirement Profile
- Provider Due Diligence Evidence Checklist
- Individual Rights Request Workflow
- Privacy Incident Coordination Playbook
- Privacy Assurance and Remediation Tracker



Day 5: Practice Connected Privacy Controls

- Exercise: Map a Connected Data Service
- Exercise: Assess Privacy Risks and Impacts
- Exercise: Design Collection, Access, and Retention Controls
- Exercise: Review a Third-Party Privacy Handoff
- Capstone: Connected Privacy Control Pack

Practical Exercises

The course uses suggested activities based on cloud services, connected products, data-sharing schemes, and customer operations.

- Suggested activity: identify processing actions, roles, purposes, transfers, and responsibility gaps across a connected service.
- Suggested activity: assess risks to individuals and prioritize control treatments using a Current and Target Profile.
- Suggested activity: test minimization, default settings, access, retention, and change controls against documented purposes.
- Suggested activity: assemble provider requirements, rights workflows, incident handoffs, assurance evidence, and remediation actions.

FAQs

Who suits connected data privacy training, and what does it assume?

Privacy, compliance, governance, risk, IT governance, audit, and operations functions suit the training; it assumes participants can document processes, data uses, controls, and ownership.

How does connected data privacy differ from technical cybersecurity training?

Connected data privacy focuses on processing purposes, individual impacts, lifecycle choices, responsibilities, rights, and assurance, while technical cybersecurity training focuses on protecting systems and responding to technical threats.

How does privacy by design support connected services?

Privacy by design embeds requirements, minimization, default settings, access rules, retention, transparency, and review gates from concept through launch, operation, change, and retirement.

How should third-party privacy risk be controlled?

Third-party privacy risk should be controlled through role clarity, documented requirements, due diligence, data-flow limits, contractual evidence, access restrictions, assurance checks, incident coordination, remediation ownership, and periodic reassessment.



What belongs in a connected data privacy risk assessment?

A connected data privacy risk assessment records processing purposes, data actions, individuals affected, roles, dependencies, potential harms, existing controls, residual risks, treatment decisions, owners, evidence, and review triggers.

Conclusion

Participants take back a Connected Privacy Control Pack containing data maps, role records, risk assessments, design requirements, lifecycle controls, provider evidence, rights workflows, incident handoffs, and assurance actions. It changes disconnected privacy tasks into an owned control system. The pack connects processing decisions, individual impacts, operational evidence, and continuous review.